RECEIVED
CENTRAL FAX CENTER
FEB 07 2007

Listing and Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method for managing access to a scrambled program, within a network comprising a first device interconnected to a second device, the method comprising:

(a) receiving said scrambled program in said first device, said scrambled program comprising a scrambled data component and a descrambling key;

(b) rebundling, in said first device, said descrambling key using a unique key associated with said first device;

(c) receiving, in said second device, said scrambled data component and said rebundled descrambling key;

(d) obtaining in said second device said descrambling key from said rebundled descrambling key; and

(e) descrambling, in said second device, said scrambled data component using said descrambling key.

2. (Previously Presented) The method of Claim 1 wherein said descrambling key is encrypted and the step of rebundling comprises:

(a) decrypting said encrypted descrambling key using a key associated with said scrambled program; and

(b) re-encrypting said descrambling key using said unique key associated with said first device to produce said rebundled descrambling key.

3. (Previously Presented) The method of Claim 2 wherein said unique key associated with said first device is a public key, said public key being located in said first device and a corresponding private key being located in said second device.

4. (Previously Presented) The method of Claim 2 wherein the step of rebundling is performed within a first smart card coupled to said first device and

the steps of obtaining and descrambling are performed within a second smart card coupled to said second device.

5. (Original) The method of Claim 1 further comprising the step of initializing said first device within said network.

6. (Previously Presented) The method of Claim 5 wherein the step of initializing comprises the step of receiving a public key from a conditional access provider, said step of receiving comprising authentication of said conditional access provider.

7. (Previously Presented) The method of Claim 5 wherein a public key is prestored in a smart card coupled to said first device or in said first device.

8. (Previously Presented) The method of Claim 1 wherein said descrambling key is encrypted using a private means if said scrambled program is received from pre-recorded media or protected by a private means if said scrambled program is received from a service provider.

9. (Cancelled)

10. (Previously Presented) A method for managing access to a scrambled program received from a service provider within a network having an access device and a presentation device, said method comprising:

(a) receiving said scrambled program in an access device, said scrambled program comprising a scrambled data component and an encrypted descrambling key;

(b) decrypting, in said access device, said encrypted descrambling key using a key associated with said service provider;

(c) re-encrypting said descrambling key, in said access device, using a public key associated with said access device;

(d) receiving, in said presentation device, said scrambled data component and said re-encrypted descrambling key;

(e) decrypting, in said presentation device, said re-encrypted descrambling key to obtain said descrambling key; and

(f) descrambling, in said presentation device, said scrambled data component using said descrambling key.

11. (Cancelled)

12. (Cancelled)

13. (Cancelled)

14. (Original) The method of claim 1, wherein the first device is an access device and wherein the second device is a presentation device.

15. (Cancelled)

16. (Cancelled)

17. (Previously Presented) An access device, comprising:

a signal input for receiving a scrambled program from a service provider, the scrambled program including a scrambled data component and an encrypted descrambling key;

a decrypting unit for obtaining the descrambling key using a key associated with the scrambled program;

an encryption unit for re-encrypting the descrambling key using a public key associated with the access device;

a signal output coupled to a digital bus for transmitting the scrambled data component and the re-encrypted descrambling key to a presentation device via the digital bus, wherein only a presentation device having a corresponding private key is able to decrypt the re-encrypted descrambling key and descramble the scrambled content.

18. (Previously Presented) The access device of claim 17, wherein the public key is periodically received from a conditional access provider.

19. (Previously Presented) The access device of claim 17, wherein the signal output authenticates the presentation device before transmitting the scrambled data component and the re-encrypted descrambling key to the presentation device.

20. (Previously Presented) The access device of claim 17, wherein the signal output transmits identification data associated with the access device and copy control information along with the re-encrypted descrambling key.

21 (New) A method for processing program signal in an apparatus coupled to an access device in a local network, comprising the steps of:

receiving, from the access device that is coupled to a service provider, a signal comprising the program signal in scrambled form and a re-encrypted descrambling information, the descrambling information being re-encrypted by the access device using key information associated with the access device;

decrypting the re-encrypted descrambling information using key information associated with the access device to obtain the descrambling key;

descrambling the program signal using the decrypted descrambling information.

22. (New) The method according to claim 21, wherein the key information corresponds to entitlement control messages, and further comprising the step of obtaining a descrambling key from the entitlement control messages, and the descrambling step comprises descrambling the program signal using the descrambling key.

23. (New) The method according to claim 21, wherein

the descrambling information is re-encrypted using a private key associated with the access device, and the decrypting step comprises decrypting the descrambling information using a public key associated with the access device.

24. (New) The method according to claim 21, further comprising the steps of:

transmitting authentication information to the access device; and

receiving key information associated with the access device from the access device following the transmission of the authentication information.